

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Naohito TAKAE (deceased) Yumiko TAKAE (heiress), et al.

Application No.: 10/644,065

Group Art Unit: 2681

Filed: August 20, 2003

Examiner: Not Yet Assigned

For: MOBILE DEVICE CONTROLLING METHOD, IC CARD UNAUTHORIZED USE
PREVENTING METHOD, PROGRAM FOR CHANGING SETTINGS OF MOBILE
DEVICE, AND PROGRAM FOR PREVENTING IC CARD FROM UNAUTHORIZED USE

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith
a certified copy of the following foreign application:

Japanese Patent Application No(s). JP 2001-57312

Filed: March 1, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

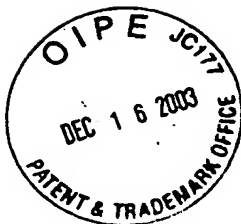
Date: Dec. 16, 2003

By: H. J. Staas

H. J. Staas

Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501



PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy
of the following application as filed with this office.

Date of Application:	March 1, 2001
Application Number:	No. 2001-057312
[ST.10/C]:	[JP2001-057312]
Applicant(s):	FUJITSU LIMITED

August 25, 2003

Commissioner,
Patent Office

Yasuo Imai (Seal)

Certificate No. 2003-3069486

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 1 年 3 月 1 日
Date of Application:

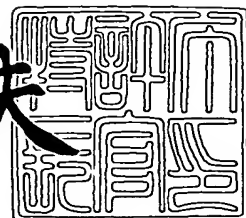
出 願 番 号 特 願 2 0 0 1 - 0 5 7 3 1 2
Application Number:
[ST. 10/C] : [J P 2 0 0 1 - 0 5 7 3 1 2]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 3 年 8 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 9 4 8 6

【書類名】 特許願

【整理番号】 0052528

【提出日】 平成13年 3月 1日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04B 7/26

【発明の名称】 携帯機器制御方法、 I C カード不正使用防止方法、携帯機器の設定を変更するプログラム及び I C カード不正使用防止のためのプログラム

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 高江 直人

【発明者】

【住所又は居所】 北海道札幌市厚別区下野幌テクノパーク 1 丁目 1 番 5 号 株式会社富士通北海道システムエンジニアリング内

【氏名】 谷 弘幸

【発明者】

【住所又は居所】 青森県青森市大字野木字山口 2 4 5 番 9 (番地なし) 株式会社富士通青森システムエンジニアリング内

【氏名】 大宮 洋行

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】**【識別番号】** 100070150**【住所又は居所】** 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデン
プレイスタワー32階**【弁理士】****【氏名又は名称】** 伊東 忠彦**【電話番号】** 03-5424-2511**【手数料の表示】****【予納台帳番号】** 002989**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9704678**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 携帯機器制御方法、ＩＣカード不正使用防止方法、携帯機器の設定を変更するプログラム及びＩＣカード不正使用防止のためのプログラム

【特許請求の範囲】

【請求項１】 携帯機器の設定を変更する携帯機器設定変更センタにおける携帯機器制御方法において、

携帯機器の設定変更の申込みを受け付ける受付ステップと、

設定変更を行う携帯機器のメールアドレスを特定するメールアドレス特定ステップと、

設定変更メールを作成するメール作成ステップとを有し、

該メール作成ステップで作成された電子メールを、前記メールアドレス特定ステップで特定されたメールアドレス先に送信して、携帯機器の設定変更を行うようにしたことを特徴とする携帯機器制御方法。

【請求項２】 請求項１記載の携帯機器制御方法において、

本体のメモリに、前記携帯機器設定変更センタ内のＩＣカード情報を管理するＩＣカード管理センタが設定したアプリケーション管理番号が登録されている場合、

前記メールアドレス特定ステップは、通知されたアプリケーション管理番号に基づいてメールアドレスを特定することを特徴とする携帯機器制御方法。

【請求項３】 携帯通信事業者における携帯機器の設定変更方法において、

ＩＣカード情報を管理するＩＣカード管理センタから設定変更を行う携帯機器のサブスクライバＩＤを受信する受信ステップと、

前記サブスクライバＩＤから、携帯機器の設定変更を行う携帯機器の通信用番号を特定するステップと、

特定された通信用番号に係る携帯機器の設定変更を行う設定変更ステップとを有することを特徴とする携帯機器の設定変更方法。

【請求項４】 携帯機器における設定変更方法において、

携帯通信事業者から送信されたメールを受信するステップと、

該受信したメールに携帯機器の設定を変更する設定変更識別子が存在するか否

かを判定するステップと、

設定変更識別子が存在する場合、自動的にメールを開くステップと、

メール内の命令によって、携帯機器本体、通信用 I C カード、決済用 I C カードの設定の内、少なくとも一つの設定を変更するステップと

を有することを特徴とする設定変更方法。

【請求項 5】 I C カード情報を管理する I C カード管理センタにおける I C カード不正使用防止方法において、

決済用 I C カードを装着した携帯機器の紛失又は盗難に合った者からの、I C カードの顧客 I D の通知を受け付ける通知受付ステップと、

前記顧客 I D に対応する番号であって、I C カード管理センタが携帯機器毎に設定したアプリケーション管理番号が格納されているデータベースの当該アプリケーション管理番号に利用停止の識別子を付与するステップと、

利用停止のアプリケーション管理番号が設定されている携帯機器を用いた決済用 I C カードの使用があった場合、当該携帯機器に対して、警告・設定変更を行うため、携帯通信事業者にサブスクライバ I D を通知するステップと

を有することを特徴とする I C カード不正使用防止方法。

【請求項 6】 携帯通信事業者における I C カード不正使用防止方法において、

I C カード情報を管理する I C カード管理センタから I C カードの不正使用を行った携帯機器のサブスクライバ I D を受信する受信ステップと、

前記サブスクライバ I D から、不正使用を行った携帯機器の通信番号を特定するステップと、

特定された携帯機器に対して、警告・設定変更を行う警告・設定変更ステップと

を有することを特徴とする I C カード不正使用防止方法。

【請求項 7】 携帯通信事業者における I C カード不正使用防止方法において、

I C カード情報を管理する I C カード管理センタから I C カードの不正使用を行った携帯機器のサブスクライバ I D を受信する受信ステップと、

前記サブスライバIDから、不正使用を行った携帯機器のメールアドレスを特定するメールアドレス特定ステップと、

前記携帯機器の設定を変更する設定変更メールを作成するメール作成ステップと、

該メール作成ステップで作成された電子メールを、前記メールアドレス特定ステップで特定されたメールアドレス先に送信して、携帯機器の設定変更を行うようにしたことを特徴とするICカード不正使用防止方法。

【請求項8】 携帯機器の設定を変更するプログラムであって、
携帯通信事業者から送信されたメールを受信するステップと、
該受信したメールに携帯機器の設定を変更する設定変更識別子が存在するか否かを判定するステップと、

設定変更識別子が存在する場合、自動的にメールを開くステップと、
メール内の命令によって、携帯機器本体、SIMカード、決済用ICカードに係る設定の内、少なくとも一つの設定を変更するステップとを
携帯機器に搭載されたコンピュータに実行させるためのプログラム。

【請求項9】 ICカード不正使用防止のためのプログラムであって、
決済用ICカードを装着した携帯機器の紛失又は盗難にあった顧客の顧客IDの通知を受け付ける通知受付ステップと、

前記顧客IDに対応する番号であって、ICカード管理センタが携帯機器毎に設定したアプリケーション管理番号が格納されているデータベースの当該アプリケーション管理番号に利用停止の識別子を付与するステップと、

利用停止のアプリケーション管理番号が記憶されている携帯機器を用いた決済用ICカードの使用があった場合、当該ICカードの使用をできないように携帯機器の設定を変更するため、携帯通信事業者にサブスライバIDを通知するステップとを

ICカード情報を管理するICカード管理センタのコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯機器制御方法、ＩＣカード不正使用防止方法、携帯機器の設定を変更するプログラム及びＩＣカード不正使用防止のためのプログラムに関する。

【0002】**【従来の技術】**

携帯電話機の利用が、従来の会話中心から、インターネットの利用へと変化している。それに伴い、有料コンテンツの閲覧料やインターネットショッピングの代金などの、通話料金以外の料金を決済する場面が多く見られるようになってきた。通常、料金や代金の支払方法としては、クレジットカードや銀行への振込・自動振込といった決済方法を利用するが、これ以外に、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カードを使った決済方法も実用化されている。

【0003】

また、携帯電話機に対するニーズも多様化してきている。これらのニーズに対応するため、電話機本体に、ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）カードと決済用ＩＣカードを装着して、通信及び決済を行う携帯電話機が普及しつつある。

【0004】

ＳＩＭカードとは、携帯機器（携帯電話機、携帯端末等）に差し込んで使う通信ＩＣカードで、携帯機器の使用者の情報（サブスクライバＩＤ等）、短縮ダイヤル、電話帳等の情報が格納されている。このＳＩＭカードには、サブスクライバＩＤが書き込まれているので、ＳＩＭカード対応の携帯機器であれば、ＳＩＭカードを差し込むことで、どの携帯機器からでも通信が可能となる。

【0005】

なお、サブスクライバＩＤとは、携帯通信事業者にサービスの利用申込みを行い、携帯通信事業者に登録されたときに、携帯通信事業者から、ＳＩＭカードに付される番号である。このサブスクライバＩＤは、ＳＩＭカードに記憶され、そのＳＩＭカードを利用して通信するときに、自動的に伝送される。

【0006】

決済用 I C カードは、携帯電話機に差し込んで使う決済用 I C カードである。この決済用 I C カードには、クレジット番号が設定されている。なお、電子マネーが格納された I C カードであってもよい。

【0007】

このような携帯電話機であれば、電話機を買い換える際、電話機全体を買い換える必要はなく、電話機本体のみを買い換えて、S I M カードは引き続き使用できるというメリットがある。また、自分の所有する携帯電話機が使用できなくても、S I M カードを他の携帯電話機に挿入して通信することが可能となり、携帯電話機の故障、電池切れでも、通信を行うことが可能となる。

【0008】

また、決済用 I C カードを組み込んでいるので、各種決済を携帯電話機を用いて行うことができる。また、電子マネーが格納された I C カードであれば、有料コンテンツの閲覧やインターネットショッピングなどの代金を決済する場合、即時決済が可能となる。

【0009】

【発明が解決しようとする課題】

上記のような S I M カードと決済用 I C カードを装着した携帯電話機を、紛失又は盗難にあった場合に問題が生じる。つまり、第三者が、その携帯電話機を使用して、通信した場合、本来の携帯電話機の所有者に課金されるという問題が生じる。同じように、第三者が、その携帯電話機を使用して、決済した場合、決済用 I C カードの名義人に料金が請求されるという問題が生じる。

【0010】

ところで、このような問題に対し、紛失又は盗難にあった S I M カードが用いられないようにするには、S I M カードに登録された電話番号による通信を不可能とする。そのためには、紛失又は盗難にあった S I M カードに登録された電話番号を携帯電話事業者に届け出る。これにより、交換装置の設定を変更し、当該 S I M カードを用いた通信ができなくなる。

【0011】

なお、紛失又は盗難にあった携帯電話機の S I M カードを用いて、通信するこ

とはできなくとも、紛失又は盗難にあった携帯電話機に、第三者の S I Mカードを挿入すれば通信が可能となる。しかし、この場合は、通信した第三者に課金されるので、課金に関しては、格別の問題は生じない。

【0012】

また、紛失又は盗難にあった携帯電話機の I Cカードの利用を制限するには、電話機本体の設定を変更しなければならない。しかしながら、従来のものでは、紛失又は盗難にあった携帯電話機に、第三者の S I Mカードを挿入して、紛失又は盗難にあった携帯電話機に挿入されていた I Cカードを用いて決済した場合は、紛失又は盗難にあった電話機本体を特定することができず、電話機（決済用 I Cカード、S I Mカードも含む）の設定の変更ができないという問題がある。

【0013】

本発明は、上記問題に鑑みなされたものであり、携帯電話機の設定変更を簡便に行うことを目的とするものである。

【0014】

【課題を解決するための手段】

上記課題を解決するために、本件発明は、以下の特徴を有する課題を解決するための手段を採用している。

【0015】

請求項 1 に記載された発明は、携帯機器（例えば、携帯電話機、P H S（Personal Handy-phone System）、携帯端末等）の設定を変更する携帯機器設定変更センタ（例えば、図 7 における携帯機器設定変更センタ 75）における携帯機器制御方法において、携帯機器の設定変更の申込みを受け付ける受付ステップ（例えば、図 3 における S T 1）と、設定変更を行う携帯機器のメールアドレスを特定するメールアドレス特定ステップ（例えば、図 3 における S T 4）と、設定変更メールを作成するメール作成ステップ（例えば、図 3 における S T 5）とを有し、該メール作成ステップで作成された電子メールを、前記メールアドレス特定ステップで特定されたメールアドレス先に送信（例えば、図 3 における S T 6）して、携帯機器の設定変更を行うようにしたことを特徴とする。

【0016】

請求項 1 記載の発明によれば、携帯機器設定変更センタが携帯機器の設定変更の申込みを受付て、携帯機器の設定変更を行うようにしたことにより、携帯電話機の設定変更を簡便に行うことができる。

【0017】

請求項 2 に記載された発明は、請求項 1 記載の携帯機器制御方法において、本体のメモリ（例えば、図 1 における決済用 IC カード 33）に、前記携帯機器設定変更センタ内の IC カード情報を管理する IC カード管理センタ（例えば、図 7 における IC カード管理センタ 71）が設定したアプリケーション管理番号が登録されている場合、前記メールアドレス特定ステップは、通知されたアプリケーション管理番号に基づいてメールアドレスを特定することを特徴とする。

請求項 2 記載の発明によれば、アプリケーション管理番号に基づいてメールアドレスを特定することにより、紛失又は盗難にあった携帯電話機に、第三者の SIM カードを挿入して、紛失又は盗難にあった携帯電話機に挿入されていた IC カードを用いて決済した場合でも、紛失又は盗難にあった携帯電話機を特定することができ、不正使用できないように紛失又は盗難にあった携帯電話機の設定変更が可能となる。

【0018】

請求項 3 に記載された発明は、携帯通信事業者における携帯機器の設定変更方法において、IC カード情報を管理する IC カード管理センタから設定変更を行う携帯機器のサブスクライバ ID を受信する受信ステップと、前記サブスクライバ ID から、携帯機器の設定変更を行う携帯機器の通信用番号（例えば、携帯電話番号、メールアドレス）を特定するステップと、特定された通信用番号に係る携帯機器の設定変更を行う設定変更ステップとを有することを特徴とする。

【0019】

請求項 3 記載の発明によれば、携帯通信事業者は、通知されたサブスクライバ ID から、携帯機器の設定変更を行う携帯機器の通信用番号を特定し、当該携帯機器に対して、設定変更を行うことができる。

【0020】

請求項 4 に記載された発明は、携帯機器における設定変更方法において、携帯

通信事業者から送信されたメールを受信するステップと、該受信したメールに携帯機器の設定を変更する設定変更識別子が存在するか否かを判定するステップと、設定変更識別子が存在する場合、自動的にメールを開くステップと、メール内の命令によって、携帯機器本体、通信用 IC カード（例えば、SIM カード）、決済用 IC カード（例えば、図 1 における決済用 IC カード 33）の設定の内、少なくとも一つの設定を変更するステップとを有することを特徴とする設定変更方法。

【0021】

請求項 4 記載の発明によれば、携帯機器において、受信したメールに携帯機器の設定を変更する設定変更識別子が存在する場合は、自動的にメールを開いて、携帯機器本体、通信用 IC カード、決済用 IC カードの設定の内、少なくとも一つの設定を変更することにより、携帯機器の携帯機器本体、通信用 IC カード、決済用 IC カードの設定が自動的に変更される。

【0022】

請求項 5 に記載された発明は、IC カード情報を管理する IC カード管理センタにおける IC カード不正使用防止方法において、決済用 IC カードを装着した携帯機器の紛失又は盗難に合った者からの、IC カードの顧客 ID の通知を受け付ける通知受付ステップと、前記顧客 ID に対応する番号であって、IC カード管理センタが携帯機器毎に設定したアプリケーション管理番号が格納されているデータベースの当該アプリケーション管理番号に利用停止の識別子を付与するステップと、利用停止のアプリケーション管理番号が設定されている携帯機器を用いた決済用 IC カードの使用があった場合、当該携帯機器に対して、警告・設定変更を行うため、携帯通信事業者にサブスクライバ ID を通知するステップとを有することを特徴とする。

【0023】

請求項 6 に記載された発明は、携帯通信事業者における IC カード不正使用防止方法において、IC カード情報を管理する IC カード管理センタから IC カードの不正使用を行った携帯機器のサブスクライバ ID を受信する受信ステップと、前記サブスクライバ ID から、不正使用を行った携帯機器の通信番号を特定す

るステップと、特定された携帯機器に対して、警告・設定変更を行う警告・設定変更ステップとを有することを特徴とする。

【0024】

請求項7に記載された発明は、携帯通信事業者におけるICカード不正使用防止方法において、ICカード情報を管理するICカード管理センタからICカードの不正使用を行った携帯機器のサブスクライバIDを受信する受信ステップと、

前記サブスクライバIDから、不正使用を行った携帯機器のメールアドレスを特定するメールアドレス特定ステップと、前記携帯機器の設定を変更する設定変更メールを作成するメール作成ステップと、該メール作成ステップで作成された電子メールを、前記メールアドレス特定ステップで特定されたメールアドレス先に送信して、携帯機器の設定変更を行うようにしたことを特徴とする。

【0025】

請求項5～7記載の発明は、請求項1～4記載の携帯機器制御方法をICカード不正使用防止方法に適用した発明である。

【0026】

請求項8に記載された発明は、携帯機器の設定を変更するプログラムであって、携帯通信事業者から送信されたメールを受信するステップと、該受信したメールに携帯機器の設定を変更する設定変更識別子が存在するか否かを判定するステップと、設定変更識別子が存在する場合、自動的にメールを開くステップと、メール内の命令によって、携帯機器本体、SIMカード、決済用ICカードに係る設定の内、少なくとも一つの設定を変更するステップとを携帯機器に搭載されたコンピュータに実行させるたのプログラム。

【0027】

請求項8記載のプログラムは、請求項1～4記載の携帯機器制御方法における携帯機器に搭載されるプログラムである。

【0028】

請求項9に記載された発明は、ICカード不正使用防止のためのプログラムであって、決済用ICカードを装着した携帯機器の紛失又は盗難にあった顧客の顧

客IDの通知を受け付ける通知受付ステップと、前記顧客IDに対応する番号であって、ICカード管理センタが携帯機器毎に設定したアプリケーション管理番号が格納されているデータベースの当該アプリケーション管理番号に利用停止の識別子を付与するステップと、利用停止のアプリケーション管理番号が記憶されている携帯機器を用いた決済用ICカードの使用があった場合、当該ICカードの使用をできないように携帯機器の設定を変更するため、携帯通信事業者にサブスクリバIDを通知するステップとをICカード情報を管理するICカード管理センタのコンピュータに実行させるためのプログラム。

【0029】

請求項9記載のプログラムは、請求項1～4記載の携帯機器制御方法におけるICカード管理センタに搭載されるプログラムである。

【0030】

【発明の実施の形態】

次に、本発明の実施の形態について図面と共に説明する。

【0031】

図1は、本発明を実施する場合の携帯電話機の構成図の一例である。図1の携帯電話機は、送受信部11、信号処理部13、音声信号インタフェース部15、入出力インタフェース部17、ICカードインタフェース部19、制御部21、記憶部23、マイク25、スピーカ27、入力装置29、出力装置31、決済用ICカード33及びSIMカード35から構成されている。

【0032】

送受信部11は、携帯電話機において、データ又は音声の信号の送受信を行う。無線部とベースバンド部とを有する。信号処理部13は、データ又は音声の信号を制御部21の制御のもとで、所定の信号の処理を行う。音声信号インタフェース部15は、音声信号をスピーカ27から出力し、音声信号をマイク25から取り入れる。入出力インタフェース部17は、データ入出力のためのインタフェースを行う。ICカードインタフェース部19は、ICカードドライバを有し、SIMカード及び決済用ICカードとのインタフェースをとる。制御部21は、送受信部11、信号処理部13、音声信号インタフェース部15、入出力イン

タフェース部 17、ICカードインタフェース部 19 及び記憶部 23 を制御し、携帯電話機を所定の機能を有する携帯電話機として機能させる。記憶部 23 には、SIMカード、決済用 ICカードの機能を実現させるソフトウェア、SIMカード、決済用 ICカードの利用のためのソフトウェア及び ICカード、SIMカードの設定変更を行うためのソフトウェア等が格納されている。入力装置 29 は、制御部 21 に対して信号入力を行う。出力装置 31 は、表示装置であって、信号処理部 13 で処理した結果等を表示する。決済用 ICカードは、例えば、IC化されたクレジットカードで、携帯機器に差し込んで使う決済用 ICカードである。この決済用 ICカードは、クレジット会社毎の ICカードであっても、複数のクレジット会社に対応した ICカードであってもよい。また、電子マネーが格納されたプリペイド形式の ICカードであってもよい。さらに、他のサービスに対応した ICカードであってもよい。SIMカードは、上述したように、携帯機器に差し込んで使う ICカードで、携帯機器の使用者の情報（サブスクライバ ID 等）、短縮ダイヤル、電話帳等の情報が格納されている。

【0033】

図 2 に、機器と機器に設定された番号を示す。決済用 ICカードには、アプリケーション管理番号が設定されている。アプリケーション管理番号は、発行される ICカード毎に、その ICカードのアプリケーションバージョン毎に、振られるユニークな番号である。例えば、複数の ICカードを利用する場合であれば、A クレジット会社の ICカードの利用に対しては、その使用者のクレジット番号と ICカードの A 社用アプリケーションバージョンに対して、ユニークな番号が、アプリケーション管理番号として付与される。同様に、B クレジット会社の ICカードの利用に対しても、その使用者のクレジット番号と ICカードの B 社用アプリケーションバージョンに対して、ユニークな番号が、アプリケーション管理番号として付与される。

【0034】

このように、アプリケーション管理番号は、利用するクレジット会社毎、利用者毎、バージョン毎に付与される。

【0035】

また、決済用 I C カードには、クレジット番号が記憶されている。決済用 I C カードが、多機能 I C カードで、その機能の一つが一枚の I C カードで複数のクレジット会社のクレジットを利用することができる場合は、この I C カード情報を管理する I C カード管理センタが設定する顧客番号であってもよい。

【0036】

図 3 を用いて、利用者の都合、業務上の都合等により、S I M カード、決済用 I C カードの設定又は、携帯電話機本体の設定を変更する手順について説明する。

【0037】

なお、図 3 は、携帯電話機の利用者、携帯電話機の電話機本体、携帯電話機の S I M カード及び決済用 I C カード、携帯通信事業者のリモートコントロールシステム／I C カード管理センタ、携帯通信事業者の交換装置間の処理フローを示す。なお、携帯通信事業者のリモートコントロールシステムは、携帯通信事業者の交換装置及び携帯電話機の設定を遠隔制御するリモートコントロールシステムであり、I C カード管理センタは、クレジット会社に係る I C カード管理センタ又は複数のクレジット会社等に係る I C カード情報を管理する I C カード管理センタである。なお、図 7 に示すように、携帯通信事業者のリモートコントロールシステム 7 3 と I C カード管理センタ 7 1 とをまとめて、携帯機器設定変更センタ 7 5 としてもよい。なお、携帯通信事業者のリモートコントロールシステム 7 3 が I C カード管理センタ 7 1 の機能を有するようにしてもよい。さらに、I C カード管理センタ 7 1 が、携帯通信事業者のリモートコントロールシステムの機能を有するようにしてもよい。

【0038】

先ず、リモートコントロールシステムは、利用者から、S I M カード、決済用 I C カードに係る設定、携帯電話機本体に係る設定の変更の申し出を受付け、その設定変更内容を確認（S T 1）する。設定内容が、交換装置 6 7 の設定変更を必要とする場合は、交換装置 6 7 の設定変更を指示する（S T 2）。交換装置 6 7 では、交換装置 6 7 の設定変更内容を登録する。例えば、特定の電話番号の使用を禁止する場合は、リモートコントロールシステムの指示に基づいて、その特

定の電話番号が使用できないように交換装置 67 に登録する (ST3)。

【0039】

次いで、設定変更すべき、SIMカード、決済用ICカード及び携帯電話機本体に係る電話機の番号やメールアドレスを特定する (ST4)。設定変更すべき、SIMカード、決済用ICカード及び携帯電話機本体に係る電話機の所有者からの依頼であれば、SIMカード及び携帯電話機本体を利用して、設定変更申込みが行われているので、設定変更すべき電話機の番号やメールアドレスは容易に判明する。

【0040】

しかしながら、携帯電話機が紛失又は盗難に合い、別の携帯電話機から、SIMカード、決済用ICカード及び携帯電話機本体の設定を変更するよう、申し込まれた場合は、簡単には、電話機の番号やメールアドレスは容易に判明しない。この場合については、図4で説明する。ここでは、設定変更すべき、SIMカード、決済用ICカード及び携帯電話機本体に係る電話機の番号やメールアドレスが判明したとして、説明を進める。

【0041】

メールアドレスが判明したので、メールフォーマットデータベース63を参照して、設定変更のメールを作成する (ST5)。なお、メールフォーマットは、図6(C)に示すように、設定変更識別子と司令部 (設定変更コマンド文) とを有する。

【0042】

図6(C)において、MEは、携帯機器本体を意味し、SIMは、SIMカード及び決済用ICカードを意味する。図6(C)では、設定変更識別子が×××1の場合は、携帯機器本体を無効とするよう設定し、設定変更識別子が×××2の場合は、SIMカード及び決済用ICカードを無効とするよう設定し、設定変更識別子が×××3の場合は、携帯機器本体、SIMカード及び決済用ICカードを無効とするよう設定する。

【0043】

次いで、作成された設定変更メールを送信する (ST6)。この設定変更メー

ルを受信した携帯電話機では、メールに設定変更識別子があるか否かを判定する（ST7）。メールに設定変更識別子がなければ、通常のメールであるので、通常通り、メールの確認を行う（ST8）。

【0044】

一方、メールに設定変更識別子が有れば、メールを自動的に開く（ST10）。通話中であっても、設定変更を優先するように設定されていれば、通信を切断してメールを開く（ST9）。

【0045】

メールを開き、メールの内容に従って、携帯機器本体、SIMカード及び決済用ICカードの設定を変更する（例えば、携帯機器本体、SIMカード及び決済用ICカードの使用できないように設定する。）（ST11、ST12）。

【0046】

図4を用いて、決済用ICカードを装着した携帯電話機が紛失又は盗難に合い、第三者が、その携帯電話機を使用して、その携帯電話機に装着されていた決済用ICカードを用いて決済した場合について説明する。

【0047】

図4は、携帯電話機の利用者、携帯電話機の電話機本体、携帯電話機のSIMカード及び決済用ICカード、携帯通信事業者のリモートコントロールシステム及びICカード管理センタ間の処理フローを示す。

【0048】

先ず、携帯電話機の利用者が、決済用ICカードの使用停止を電話等で行う（ST21）。そのとき、利用者は、決済用ICカードのクレジット番号（決済用ICカードが、多機能ICカードで、その機能の一つが一枚のICカードで複数のクレジット会社のクレジット等を利用することができる場合は、このICカード情報を管理するICカード管理センタが設定する顧客番号であってもよい。）と氏名を通知する。

【0049】

ICカード管理センタでは、利用者認証データベース59を参照して、利用者の認証を行う（ST22）。利用者認証データベース59には、図6（A）に示

すように、クレジット番号（顧客番号）と氏名が対応して格納されている。

【0050】

次いで、アプリケーション管理情報データベース 61 の利用状況識別子を利用停止に設定する。アプリケーション管理情報データベース 61 には、図 6（B）に示すように、アプリケーション管理情報が格納されている。紛失又は盗難に合った利用者のクレジット番号（顧客番号）のアプリケーション管理番号の利用状況識別子を利用停止に設定する。例えば、図 6（B）では、×××××2 の利用状況識別子を利用停止に設定する。

【0051】

このように設定した後、携帯電話機を拾った第三者が、この携帯電話機に第三者の SIM カードを装着し、拾った携帯電話機の決済用 IC カードを利用した（ST25）。そのとき、携帯電話機は、IC カード管理センタに IC カードの利用の認定依頼を行う（ST26）。

【0052】

IC カードの利用の認定依頼において、携帯電話機（拾った携帯電話機）に装着された決済用 IC カードに記憶されているアプリケーション管理番号、SIM カード（第三者の SIM カード）に設定されているサブスライバ ID 及び決済用 IC カード（拾った携帯電話機に装着されていた IC カード）のクレジット番号（顧客番号）が、IC カード管理センタに送信される。

【0053】

IC カード管理センタでは、アプリケーション管理番号及びクレジット番号（顧客番号）に基づいて、アプリケーション管理情報データベース 61 の利用状況識別子を参照する（ST27）。このとき、アプリケーション管理番号の利用状況識別子が利用停止に設定されていなければ、IC カードの利用を許可する（ST29）。また、このとき、アプリケーション管理番号の利用状況識別子が利用停止に設定されていれば、IC カードの利用を許可せずに、携帯通信事業者に、サブスライバ ID を通知する（ST30）。携帯通信事業者は、携帯電話管理情報データベース 65 を参照して、サブスライバ ID から、携帯電話機の電話番号及びメールアドレスを特定する（ST31）。図 6（D）に携帯電話管理情

報データベースの例を示す。

【0054】

この後、携帯通信事業者は、先に説明した図4に基づく処理を行う。

【0055】

図5を用いて、ICカード管理センタの例について説明する。ICカード管理センタは、一つのクレジット会社に係るICカード管理センタであっても、又は複数のクレジット会社に係るICカード情報を管理するICカード管理センタであってもよく、アプリケーション提供会社、チケット販売会社と提携していてもよい。

【0056】

図5のICカード管理センタは、複数のクレジット会社に係るICカード情報を管理するICカード管理センタであって、アプリケーション提供会社、チケット販売会社と提携しているICカード管理センタの例である。

【0057】

図5では、通信インタフェース部41、ユーザ管理部43、アプリケーション管理部45、カード管理部47、カード発行種管理部49、発行履歴管理部51を有する。

【0058】

通信インタフェース部41は、利用者53、携帯通信事業者55及び複数のクレジット会社、アプリケーション提供会社、チケット販売会社等との通信のためのインタフェースを取る。ユーザ管理部43は、ユーザの管理を行う。例えば、ユーザの登録、利用者認定情報データベースを参照して、利用者の認定等を行う。アプリケーション管理部45は、アプリケーションの管理を行う。例えば、アプリケーションのバージョンの管理、アプリケーション管理情報データベース61の利用状況識別子の設定、アプリケーション管理情報データベースを参照して、ICカードの利用可能か否かの処理を行う。カード管理部47は、ICカードの発行主体、内容等を管理している。カード発行種管理部49は、ICカード別にその発行された種類を管理している。発行履歴管理部51は、ICカード別にその発行履歴を管理している。

【0059】

以上の通り、本発明の実施の形態によれば、携帯機器で使用されるＩＣカードを紛失又は盗難に合った者が、センタにＩＣカードを紛失又は盗難を申し出た場合、単に当該ＩＣカードによる、決済を行わないだけでなく、携帯機器の設定を変更して、当該ＩＣカードが利用できないようにすることができるので、より安全性が高まる。

【0060】

また、紛失又は盗難に合ったＩＣカードが、複数の会社の決済が可能であったり、決済以外の機能を有している場合、センタにＩＣカードを紛失又は盗難を申し出るだけで、当該ＩＣカードが利用できないようにすることができるので、紛失又は盗難時の対応が簡便になる。なお、従来では、ＩＣカードに関係する全ての企業に連絡する必要があったが、本発明の実施の形態では、携帯機器設定変更センタ又はＩＣカード管理センタに連絡するだけでよい。

【0061】**【発明の効果】**

上述の如く本発明によれば、携帯機器を紛失した場合等に起こり得る被害（ＩＣカードの不正使用による損害等）を事前に抑止できるようになる。

【0062】

また、不正利用しようとした第三者の電話番号等が分かるため、警告を発したり、ペナルティを課す等の対応をとることが可能となる。

【0063】

また、紛失又は盗難にあった携帯電話機に第三者のＳＩＭカードを挿入して、紛失又は盗難にあった携帯電話機に挿入されていたＩＣカードを用いて決済した場合でも、紛失又は盗難にあった携帯電話機を特定することが可能となる。

【0064】**【図面の簡単な説明】****【図１】**

本発明を実施する場合の携帯電話機の構成図の一例である。

【図２】

機器と機器に設定された番号の例を示す。

【図 3】

SIMカード、決済用ICカード及び携帯電話機本体の設定を変更する手順の例を説明するための図である。

【図 4】

決済用ICカードを装着した携帯電話機が紛失又は盗難に合い、第三者が、その携帯電話機を使用して、その携帯電話機に装着されていた決済用ICカードを用いて決済した場合の対応処理フローを示す。

【図 5】

ICカード管理センタの構成例を説明するための図である。

【図 6】

データベースに格納される情報のデータ構造の例を説明するための図である。

【図 7】

携帯機器設定変更センタの例を説明するための図である。

【符号の説明】

- 11 送受信部
- 13 信号処理部
- 15 音声信号インタフェース部
- 17 入出力インタフェース部
- 19 ICカードインタフェース部
- 21 制御部
- 23 記憶部
- 25 マイク
- 27 スピーカ
- 29 入力装置
- 31 出力装置
- 33 決済用ICカード
- 35 SIMカード
- 41 通信インタフェース部

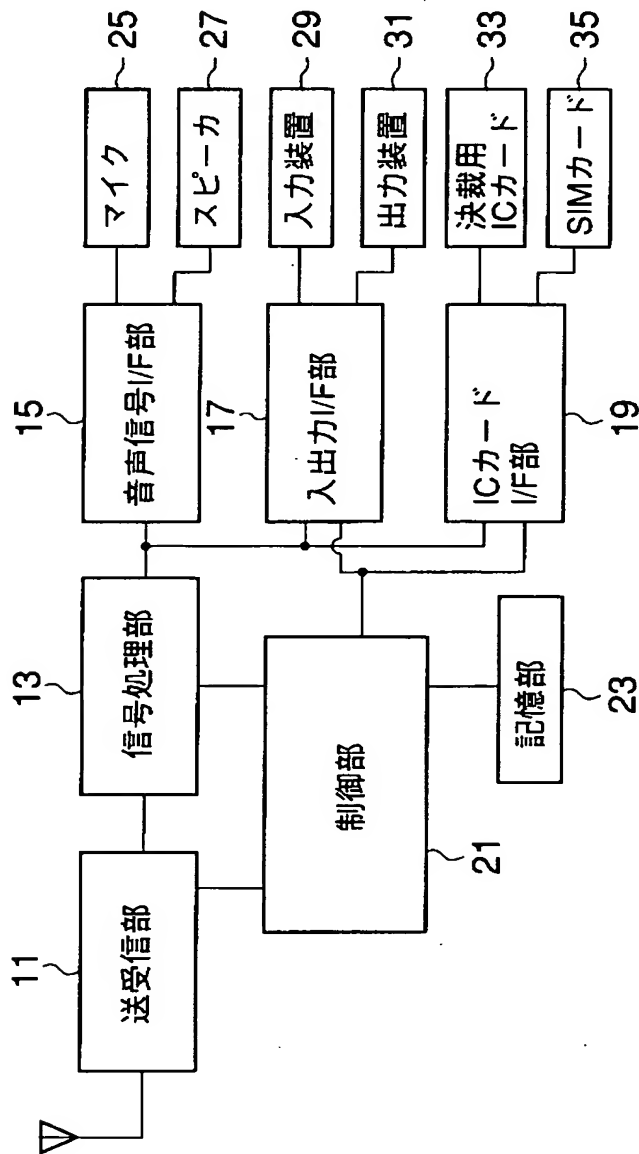
- 4 3 ユーザ管理部
- 4 5 アプリケーション管理部
- 4 7 カード管理部
- 4 9 カード発行種管理部
- 5 1 発行履歴管理部
- 5 3 利用者
- 5 5 携帯通信事業者
- 5 7 複数のクレジット会社、アプリケーション提供会社、チケット販売会社等
- 5 9 利用者認定情報データベース
- 6 1 アプリケーション管理情報データベース
- 6 3 メールフォーマットデータベース
- 6 5 携帯電話管理情報データベース
- 6 7 交換装置
- 7 1 ICカード管理センタ
- 7 3 リモートコントロールシステム
- 7 5 携帯機器設定変更センタ

【書類名】

図面

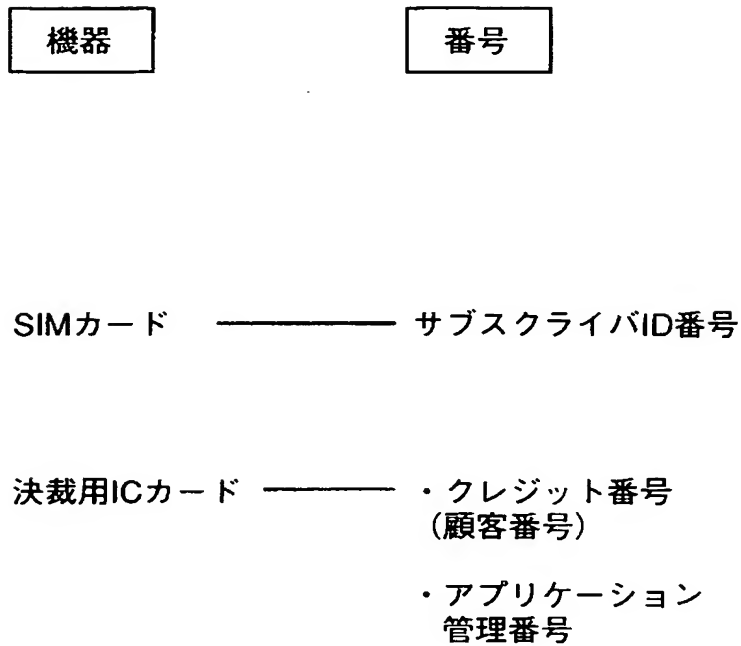
【図 1】

本発明を実施する場合の携帯電話機の構成の一例



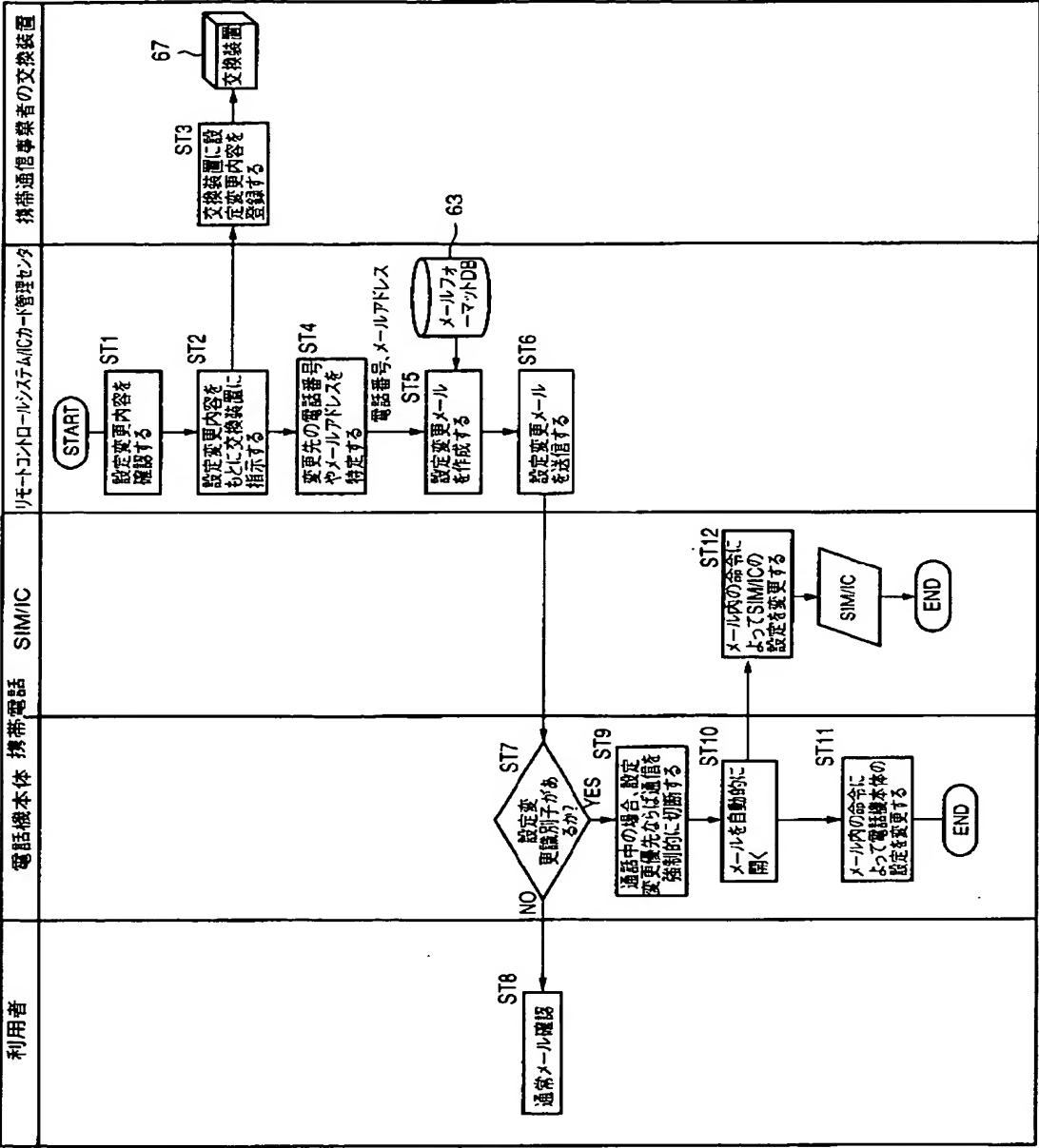
【図 2】

機器と機器に設定された番号の例を示す



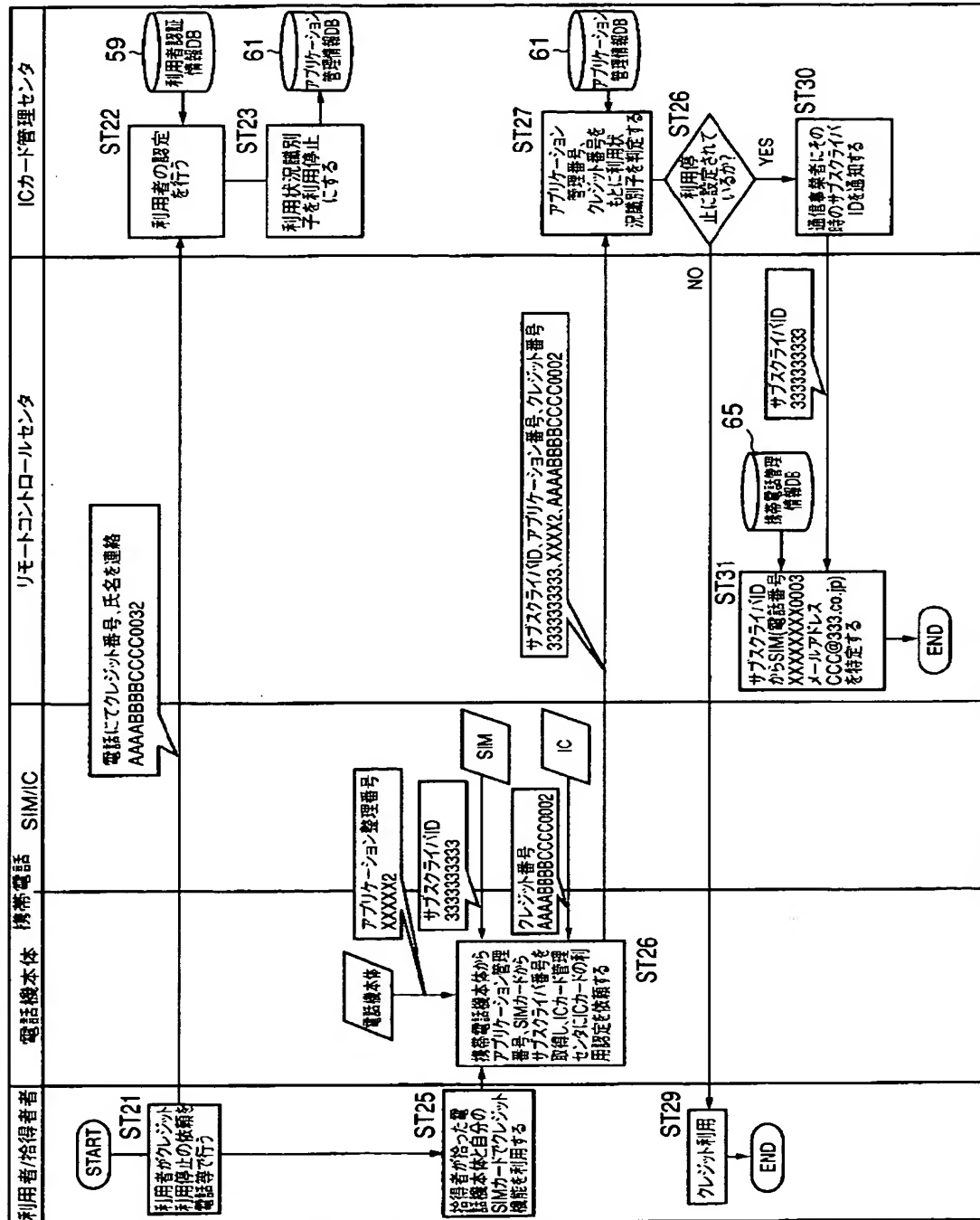
【図 3】

SIMカード、決済用IDカード及び携帯電話機本体の設定を変更する手順の例を説明するための図



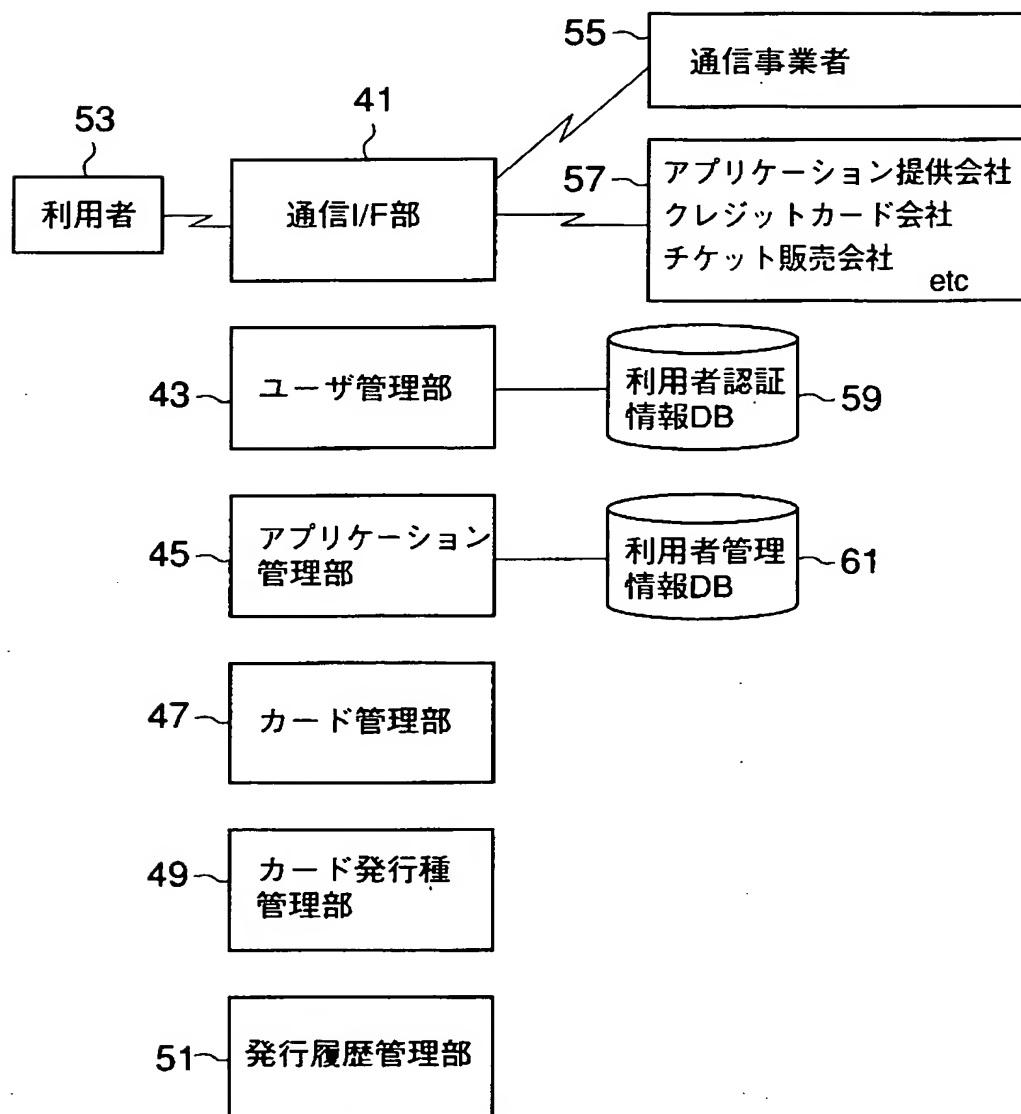
【図 4】

決済用ICカードを装着した携帯電話機が紛失又は盗難に合い、第三者が、その携帯電話機を使用して、その携帯電話機に装着されていた決済用ICカードを用いて決済した場合の対応処理フロー



【図 5】

ICカード管理センタの構成例を説明するための図



【図 6】

データベースに格納される情報のデータ構造の例を説明するための図

利用者認証情報

No.	クレジット番号(顧客番号)	氏名
1	AAAABBBBCCCC0001	青森太郎
2	AAAABBBBCCCC0002	青森次郎

(A)

アプリケーション管理情報

No.	アプリケーション管理番号	クレジット番号(顧客番号)	利用状況識別子	サブスクライバID
1	XXXXX1	AAAABBBBCCCC0001	利用可	1111
2	XXXXX2	AAAABBBBCCCC0002	利用停止	2222

(B)

メールフォーマット

No.	設定変更識別子	命令部(設定変更コマンド文)
1	XXX1	電話機本体ロック命令
2	XXX2	SIMロック命令
3	XXX3	電話機本体, SIMロック命令

(C)

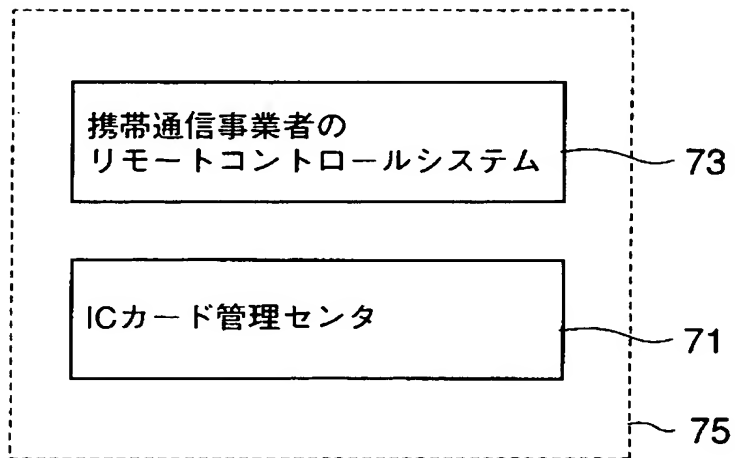
携帯電話管理情報

No.	サブスクライバID	電話番号	メールアドレス
1	1111111111	XXXXXXXXXX0001	aaa@111.co.jp
2	2222222222	XXXXXXXXXX0002	bbb@222.co.jp
3	3333333333	XXXXXXXXXX0003	ccc@333.co.jp

(D)

【図 7】

携帯機器設定変更センタの例を説明するための図



【書類名】 要約書

【要約】

【課題】 携帯電話機の設定変更を簡便に行うことを目的とする。

【解決手段】 SIMカードと決済用ICカードが装着可能な携帯機器の設定を変更する携帯機器制御方法である。

本発明は、携帯機器の設定変更の申込みを受け付けて確認するステップ（ST1）と、設定変更を行う携帯機器のメールアドレスを特定するメールアドレス特定ステップ（ST4）と、設定変更メールを作成するメール作成ステップ（ST5）とを有し、該メール作成ステップで作成された電子メールを、前記メールアドレス特定ステップで特定されたメールアドレス先に送信して（ST6）、携帯機器の設定変更を行う。

【選択図】 図3

特願 2 0 0 1 - 0 5 7 3 1 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中 1 0 1 5 番地

氏 名

富士通株式会社

2. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社